DEPARTMENT OF THE NAVY
BOARD OF INSPECTION AND SURVEY
2600 TARAWA COURT SUITE 250
VIRGINIA BEACH, VA 23459-3295

INSURVINST 4730.27
25 July 2012

INSURV INSTRUCTION 4730.27

From: PRESIDENT BOARD OF INSPECTION AND SURVEY

Subj: INFORMATION SYSTEMS MATERIAL AND SECURITY INSPECTION

1. Purpose. To establish INSURV policy for evaluating the material condition and associated administrative processes of ship and submarine network-based information systems.

2. Discussion. INSURV will focus on computer network (NIPR/SIPR/SCI) information system material condition, system administration, security and directive compliance in order to assess whether the information systems are properly installed, configured and managed to adequately meet information assurance requirements in support of the platform's mission. The demonstration of the network security systems and associated programs such as physical and personnel security compliance will be included as part of each ship Material Inspection (MI), ship Final Contract Trial (FCT), and submarine Combined Trial (CT), and will include inspection of specific systems, associated software, and administrative programs for compliance with Computer Network Defense (CND) Directives. The following programs, equipment, systems, and documentation pertinent to network (NIPR/SIPR/SCI) security will be demonstrated/assessed:

a. Cyber Security Work Force (qualifications).

b. Site Accreditation & Management.

c. Computer Network Defense.

d. Information Assurance Vulnerability Management.

e. USB Policy and Detection.

f. Traditional Security (Security-in-Depth & space).

g. Intrusion Detection Systems (doors & scuttles).

h. Network Security.

i. Protected Distribution Systems (PDS).

j. Directive compliance (CTO, NTD, FAM).

k. Contingency Plans (Testing & Documentation).

l. Cross-Domain Solution Systems.

4. Policy. The inspection will be conducted on all in-service ships and submarines during MIs, FCTs, and CTs.

5. Pre-Inspection Requirement:

a. The ship shall provide the following items as part of the pre-inspection workbook:

(1) Command Security instruction.

(2) Information Assurance instructions/policies.

(3) Network failover test procedure(s) for mission critical systems that will demonstrate the integrity of the system state with the loss of a redundant core switch or equipment.

b. On day one the ship shall provide the IS uniformed inspector with a binder containing the following items:

(1) Entire accreditation package.

(2) Commanding Officer's Designated Accrediting Authority (DAA) course certificate.

(3) Letters of designation for IA Manager (IAM) & Security Manager.

(4) Appointment letters for CSWF personnel.

(5) IA Workforce billet status report from Total Workforce Management Services (TWMS) website.

(6) Approved CSWF certification waivers.

(7) Network topology drawings.

(8) Information Asset inventory (hardware & software).

(9) List of Program of Record (POR) and non-POR systems.

(10) List of Platform IT systems.

(11) Authorization to Operate (ATO) letters.

(12) Platform IT (PIT) Risk Approval (PRA) & ATO letters.

(13) PDS Certification letter.

(14) Blue Team Assessment results from latest visit.

(15) Signed User agreement forms (locator card is preferred vice copies of all forms).

(16) List of designated Secure Rooms, Vaults, Controlled Access Areas, and Restricted Assess Areas.

(17) List of GSA safes.

(18) List of shredders, pulverizers and disintegrators.

(19) Completed System Operational Verification Test (SOVT) procedures (locator card).

(20) Hardcopy of open software trouble tickets.

c. In addition, the ship is encouraged to have reviewed and implemented the best practices outlined in the NAVYCYBERFOR Commander's Cyber Security and Information Assurance Handbook and its associated enclosures.

d. Ships shall ensure compliance with Preventive Maintenance System checks as applicable for the network variant and computer network defense system installed.

e. Further, to ensure all network scans touch 100% of the NIPR/SIPR/SCI networks, as applicable, every assigned asset

shall be connected to the network and energized from day one through the end of the inspection.

6. Information Systems Security Check Procedures. Required inspection checklists can be found on the INSURV website (http://www.public.navy.mil/fltfor/insurv/Pages/default). The ship shall ensure the system administrators (SA) and Information Assurance Manger (IAM) are available to demonstrate all checklist items. Observation of ship behavior with regard to cyber, physical and personnel security will be ongoing until the Board departs.

7. INSURV will continue the inspection process for other Information Systems, both tactical and non-tactical, to include, but not limited to, NTCSS, NIAPS, GCCS-M, JTT, and SSES/TSCI systems. Accordingly, ships shall ensure appropriate SA and privileged user personnel are designated and available to demonstrate all of these Information Systems and that all passwords, logins and permissions are in place to assure the proper level of access for demonstration of these systems.

8. The Commanding Officer is ultimately responsible for managing the cyber readiness of his/her command. At no time will the Commanding Officer's Cyber Security posture be compromised.

//s//
R. O. WRAY

Distribution:
CNO
ASSTSECNAV RDA WASHINGTON DC
COMUSFF
COMPACFLT PEARL HARBOR HI
COMNCF
COMFCC
COMNNWC
COMSECONDFLT
COMTHIRDFLT
COMNAVSURFOR SAN DIEGO CA
COMNAVSURFLANT NORFOLK VA

COMNAVAIRFOR SAN DIEGO CA
COMNAVAIRLANT NORFOLK VA
COMSUBLANT NORFOLK VA
COMSUBPAC PEARL HARBOR HI
COMNAVSURFGRU MIDPAC
COMSURFWARDEVGRU LITTLE CREEK VA/ CDS-26
CENSURFCOMBATSYS DET EAST NORFOLK VA
COMNAVSEASYSCOM WASHINGTON DC
PEO SHIPS WASHINGTON DC
PEO SUBS WASHINGTON DC
PEO C4I SAN DIEGO CA
PEO IWS WASHINGTON DC
NAVSURFWARCENDIV DAHLGREN VA
CENSURFCOMBATSYS DAHLGREN VA
COMSPAWARSYSCOM SAN DIEGO CA
NAVSURFWARCENDIV PORT HUENEME CA
SPAWARSYSCEN ATLANTIC CHARLESTON SC
SPAWARSYSCEN PACIFIC DET GROUP TWO NORFOLK VA
SPAWARSYSCEN PACIFIC SAN DIEGO CA
AEGIS TECHREP MOORESTOWN NJ
USFF N43